UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,559	04/06/2001	Osamu Shibata	29288.0300	6490

20322 7590 08/06/2007

SNELL & WILMER L.L.P. (Main)
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
08/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/828,559	SHIBATA ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: attachment

DETAILED ACTION

1. This action is responsive to communications: application, filed 4/6/2001; amendment filed 5/24/2007.

2. Claims 1-49 are pending in the case.

Response to Arguments

3. Applicant's amendment to claims 1 and 14 clarifies the antecedent basis issues, and their argument has been persuasive. Accordingly, the Objection to clams 1, 14, 26 and 37 is hereby withdrawn.

4. Applicant's argument to traverse the 103 rejection to claims 1-47 is found non persuasive for the following reasons:

Applicant argues: "Applicants assert that neither item 14 nor item 131 of Ishibashi generates a contents key Kcd based on a copy control code. In particular, Ishibashi simply discloses that a copy control code is added to the content key Kcd (e.g., col. 6, lines 10-12 of Ishibashi)." However, the combination of the K_{cd} and the copy control code is an item that is generated based on the copy control code. That item is later encrypted by an encryption key (see col. 6 lines 1-20). Applicant further argues: "In addition, Ishibashi also clearly

states that the copy control code and the previously generated content key Kcd can be encrypted separately and transmitted separately without departing from the invention (e.g., col. 13, lines 53-54)." The fact that Ishibashi teaches the option to encrypt K_{cd} and copy control code separately shows that at another point K_{cd} and the copy control code where combined in one item. That one item is more clearly depicted in Fig. 10 and associated text as $K_{cd}{}^{cx}$. Note also that col. 11 lines 5-8 states that item 133 **encrypts** the copy control code by adding it to K_{cd}. Therefore, the added code is not just a mere addition in the sense of to separate fields that are concatenated. If they were, the copy control code would not be encrypted. Therefore, $K_{cd}{}^{cx}$ is an item that is generated by device 130, which is a content decryption key, and is generated based on the copy control code. Note that using $K_{cd}{}^{cx}$, item 200 decrypts the content and performs copy control.

Applicant also argues that Ishibashi does not teach "a second contents key generation section" based on the same argument that the generated key is not based on the copy control code. However, as discussed above, item 130 generates a key based on the copy control code. Therefore, Ishibashi does teach "a second contents key generation section".

Applicant further argues against the motivation to implement the functionality of copy control at item 10 based on the copy control functionality taught based on item 100. Applicant argues: "However, Ishibashi has not provided the motivation to impose such restriction on the server-side content provider 10. In particular, the server-side content provider

10 holds content data such as image, music, program, etc, and supplies the content data to a user at the user-side information processor 100 (e.g., col. 3, lines 43-55). Therefore, it is undesirable for the server-side content provider 10 to be restricted in regards to the copying of the content data. Accordingly, one skilled in the art would not have modified the server-side content provider 10 to perform the same copy control process carried out by the user-side information processor 100 as alleged by the Examiner." However, the copy control function requires cooperation between the server side 10 and the user side 100. Ishibashi teaches that the copy control code is changed based on the number of copies made by each user. Fig. 8 shows an example of 2 users in items 100 and 200. Therefore, the total number of allowed copied must be determined, and provisioned in the copy control code. Indeed the content provider is interested in determining how many copies are to be made, and therefore, there is a definite motivation to implement the copy control functionality at the server side.

Applicant argues that claims 2-47 are differentiated from the prior art for the same reasons discussed above. However, the reasons discussed above have been found non persuasive.

Applicant further argues that Examiner's explanation regarding the limitation of the third encryption and decryption section fails to specify the details of the limitations. Applicant argues: "We note that the Examiner fails to specifically state the corresponding components disclosed by Ishibashi for such features of claim 1. In particular, Applicants respectfully assert

that the Examiner simply generally states that the copy control code is buried in the content data and all the communication between devices is encrypted by a session key." However, Examiner's explanation about the details of said limitations is far mote than a simple general statement, as it includes references to several parts of Ishibashi and an explanation that the time varying key is represented by a session key (see the Office Action dated 2/27/07, page 7). Note also that when all communication between devices is encrypted, it means that there is an encryption element at the sending side, and a decryption element at the receiving side.

Applicant also argues that Examiner did not provide specific support for the limitations of encrypting the first decryption limitation and updating the second decryption limitation by first decryption limitation. However, Examiner has explained, by referencing relevant parts of Ishibashi (see page 6 of the Office Action dated 2/27/07), that the copy control code and its updating process teach the encryption of the first decryption limitation and the updating of the second decryption limitation by the first decryption limitation.

Applicant has added new claims 48 and 49. The new claims are rejected as outlined in the next section.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi (U.S. Patent No. 6,728,379 B1, filed July 28, 1999).

6.1. As per claim 1, Ishibashi is directed to a copyright protection system (column 1 line 22 to 25) comprising: an encryption device (item 10 and associated text. Items 100 and 200 also perform encryption) and a decryption device (Information Processors 100 and 200 both perform decryption), wherein cryptographic communication is performed between the encryption device and the decryption device (Figures 2 and 3 and the associated texts) using a contents key (Kce and Kcd as shown in Figures and associated text. Also note that public key encryption, (which uses separate keys for encryption and decryption) can be replaced by private (symmetric) key encryption, which uses one key for both encryption and decryption, as indicated in col. 4 line 34 to 42), wherein the encryption device includes a contents storage section for storing contents (item 11 of Fig. 8 and associated text), a first contents key generation section for generating the contents key (item 14 of Fig. 8 and associated text, also see column 4 line 24 to 33) based on a second decryption limitation obtained by updating a first decryption limitation (column 6 line 1 to 20 discloses SCMS as an example system of a copy control scheme that uses control codes in set in the content and the associated encryption keys for copy control. Also note that the process of updating the content key based on the copy control code and client usage and purchase of content is clearly

disclosed in col. 9 line 52 to col. 13 line 60. The process is explained within item 100, but it would have been obvious to a person skilled in art to perform the same in item 10 (content provider), where the content key is generated. The motivation is to allow the content provider to control the copying of the content), and a first encryption section for encrypting the contents using the contents key (item 13 Fig. 8) and outputting the encrypted contents (item 15 Fig. 8), and wherein the decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation (item 131 of Fig. 8 generates Kcd, which is used to decrypt the content. As the content was encrypted based on a copy control scheme, namely SCMS, the copy control code was updated and embedded in the content or the key (see column 10 line 53 to 66 and also column 13 line 47 to 60), accordingly) and a first decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section (item 136 of Fig. 8 and associated text), wherein the encryption device further includes a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device (the copy control data (encryption limitation) is buried in content data (see, for example, col. 1 line 1-5), and all the communication between devices is encrypted by a session key (see, for example, col. 9 line 3-10, or col. 10 line 60 to col. 13 line 47), which is a time-varying key), and the decryption device further includes a third decryption section for decrypting the second encrypted decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation (all

communication is encrypted by a session key as explained above. Also see Fig. 6 and associated text).

6.2. As per claim 2, Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 12 line 4 to 15), and a second encryption section for encrypting the second decryption limitation using a time-varying key (column 12 line 33 to 43), and outputting the first encrypted decryption limitation, wherein the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second encryption section using the time-varying key to generate the second decryption limitation, wherein the first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section (column 13 line 15 to 26. Note that the Content provider and the information system 100 also perform the SCMS method for inclusion of the copy control code to limit number of allowable copies at item 100. Therefore, content encryption and key generation at the content provider also involves updating encryption keys based on the control code and in accordance with the copy rights updated at the information center.).

6.3. As per claim 3, Ishibashi is directed to a copyright protection system according to claim 2, wherein the encryption device further includes a first common key storage

section for storing a common key (column 9 line 4 to 10 discloses a mutual authentication between all elements in Fig. 8. Furthermore, the said mutual authentication is described in column 7 lines 33 to 65. Therefore, the content provider executes a mutual authentication method, namely ISO/IEC 9798-3, which will require establishment of a common key, and a location for storage), a decryption limitation storage section for storing the first decryption limitation (as described in response to claim 2, the content provider performs SCMS in association with the item 100 to establish a copy code, and therefore stores a copy code, which is updated in sync with item 100), a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second random number transferred from the decryption device, a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section (random number generation and exchange between two parties performing mutual authentication, and establishment of a session key, are part of a mutual authentication method, namely ISO/IEC 9798-3 performed between the content provider and item 100, as described in Fig. 6 and the associated text, and also column 5 lines 5 to 21), and wherein the decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device

using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section (again, item 100 performs SCMS for receiving the copy codes using a session key obtained thorough a mutual authentication).

6.4. As per claims 4 and 5 Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 6 lines 1 to 20), and a second contents key generation section for generating the contents key based on the second decryption limitation updated by the first decryption limitation updating section (column 10 line 42 to column 11 line 9), wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section, the first contents key generation section generates the contents key based on the second decryption limitation updated by the first decryption limitation updating section (the content provider and Information Processing Unit 200 both perform SCMS and implement copy code updating and secure exchange of the copy code).

6.5. As per claim 6, Ishibashi is directed to a copyright protection system according to claim 5, wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance (column 10 lines 9 to 26 discloses the case when the content decryption and distribution decryption keys are supplied by the Key Distribution Center, item 30, and therefore are supplied in advanced), the first contents key generation section generates the contents key from the second decryption limitation, and the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section (see responses to claim 3 and 4).

6.7. As per claim 7, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key (time varying keys, and their generation is disclosed in method ISO/IEC 9798-3 for mutual authentication. See column 7 line 37).

6.8. As per claim 8, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key (see response to claims 45 and 5).

6.9. As per claim 9, Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key(as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Sequence key generation is a well-known method to synchronize receiver and transmitter engaged in secure data transmission and improve the strength of encryption, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 9.5). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

6.10. As per claim 10, 11, 12 Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and

second random numbers, the common key, and the respective data sequence key (see response to claims 9, 3 and 4).

6.10. As per claim 13, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol (as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Challenge-response is a well-known method to establish mutual authentication between parties, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 3.2, page 54). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

6.14. As per claim 14, Ishibashi is directed to an encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising: a contents storage section for storing contents (fig. 8 item 11); a second encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device (see response to claim 1); a contents key generation section (item 14) for generating the contents key based on a second decryption limitation obtained by

updating a first decryption limitation (column 6 lines 1 to 20, column 10 lines 53 to 66, and column 12 lines 25 to 44 disclose Ishibashi's use of SCMS, which controls the number of copies made from copyright protected material by updating limitations of copy codes in the content data and keys); and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents (item 16).

6.15. As per claims 15 to 25 Ishibashi is directed to an encryption device according to claim 14 (item 100 in Fig. 8 discloses both encryption and decryption devices, as it receives the encrypted content data from item 10, decrypts it to extract the content, and re-encrypts it in accordance with the copy control code (copy limitation) and sends it to item 200 (another Information Center), which perform decryption. As described in responses to claims 1 to 13, this process is secured by mutual authentication between items 10, 100, 200 and other elements in Fig. 8. Mutual authentication involves the use of encryption techniques such as time-varying keys, random number generation and use for key generation, challenge–response protocol, data segmentation, etc. Ishibashi also discloses SCMS method for copy control. In the following, the encryption device is disclosed by item 100, and decryption device is disclosed by item 200. Item 100 does disclose all the elements of claim 14, as it includes and encryption section, and performs SCMS to update the copy code sent to item 200), further including a decryption section for decrypting the first encrypted decryption limitation transferred from the decryption device (item 131) using the time-varying key to generate the second decryption limitation, and the contents key generation section generates the contents

key based on the second decryption limitation generated by the decryption device (item 133 and the associated text, also see responses to claims 1 to 14).

6.16. As per claim 26, Ishibashi is directed to a decryption device (Fig. 8 item 100 or 200) for performing cryptographic communication in association with an encryption device (item 100 or 10) using a contents key, comprising: a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20); a contents key generation section for generating the contents key from a second decryption limitation (item 231 generates the key to decrypt the content decryption key, which in accordance with SMCS includes a copy code (decryption limitation); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 236 and the associated text).

6.17. As per claims 27 to 36 Ishibashi is directed to a decryption device according to claim 26, further including an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption

limitation (item 200 performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20).

6.18. As per claims 37 to 47, Ishibashi is directed to a recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device (Fig. 8 item 100), a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20); using a contents key, wherein: the program causes the computer to function as: a contents key generation section for generating the contents key from a second decryption limitation (item 133, as described in response to claim 15); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 131 as explained in response to claim 15, and response to claims 1 to 16).

6.19. As per claim 48, Ishibashi is directed to a copyright protection system according to claim 1, wherein the first and second contents key generation sections generate the contents key by using an algorithm which uses the second decryption limitation as an

input (as discussed in the Response to Arguments section above, Ishibashi teaches a key ($K_{cd}{}^{cx}$), which is an encryption key generated based on the copy control code (second decryption limitation). Therefore the content key generator generates the key with the second decryption limitation as an input).

6.20. As per claim 49, Ishibashi is directed to a copyright protection system according to claim 48, but Ishibashi does not disclose details such as the encryption technique to be used to perform different encryption processes, as the details of many encryption algorithms and techniques were well known in art at the time of his invention. Therefore, Ishibashi does not explicitly specify the one-way function as the algorithm to perform encryption.

Examiner takes the official notice that One-way function was a well known and widely practiced encryption technique at the time of invention. Therefore, it would have been obvious to the one skilled in art to use the One-way function as the algorithm to generate the key. The motivation to do so would have been to protect the key generation algorithm by using a one-way function, which makes it difficult for the hackers to discover the elements of the key generation process by analyzing the key.

As an example of prior art, please see Applied Cryptography (as identified in response to claim 9) sections 2.4 and 8.1.

Conclusion

7. No new ground of rejection is included for claims 1-47. Applicant's amendment to claims 48 and 49 necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

he is with the one-way function.) For public-key cryptography, we need something else (although there are cryptographic applications for one-way functions—see Section 3.2).

A **trapdoor one-way function** is a special type of one-way function, one with a secret trapdoor. It is easy to compute in one direction and hard to compute in the other direction. But, if you know the secret, you can easily compute the function in the other direction. That is, it is easy to compute $f(x)$ given x, and hard to compute x given $f(x)$. However, there is some secret information, y, such that given $f(x)$ and y it is easy to compute x.

Taking a watch apart is a good example of a trap-door one-way function. It is easy to disassemble a watch into hundreds of minuscule pieces. It is very difficult to put those tiny pieces back together into a working watch. However, with the secret information—the assembly instructions of the watch—it is much easier to put the watch back together.

2.4 ONE-WAY HASH FUNCTIONS

A **one-way hash function** has many names: compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and manipulation detection code (MDC). Whatever you call it, it is central to modern cryptography. One-way hash functions are another building block for many protocols.

Hash functions have been used in computer science for a long time. A hash function is a function, mathematical or otherwise, that takes a variable-length input string (called a **pre-image**) and converts it to a fixed-length (generally smaller) output string (called a **hash value**). A simple hash function would be a function that takes pre-image and returns a byte consisting of the XOR of all the input bytes.

The point here is to fingerprint the pre-image: to produce a value that indicates whether a candidate pre-image is likely to be the same as the real pre-image. Because hash functions are typically many-to-one, we cannot use them to determine with certainty that the two strings are equal, but we can use them to get a reasonable assurance of accuracy.

A one-way hash function is a hash function that works in one direction: It is easy to compute a hash value from pre-image, but it is hard to generate a pre-image that hashes to a particular value. The hash function previously mentioned is not one-way: Given a particular byte value, it is trivial to generate a string of bytes whose XOR is that value. You can't do that with a one-way hash function. A good one-way hash function is also **collision-free**: It is hard to generate two pre-images with the same hash value.

The hash function is public; there's no secrecy to the process. The security of a one-way hash function is its one-wayness. The output is not dependent on the input in any discernible way. A single bit change in the pre-image changes, on the average, half of the bits in the hash value. Given a hash value, it is computationally unfeasible to find a pre-image that hashes to that value.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

7/25/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Think of it as a way of fingerprinting files. If you want to verify that someone has a particular file (that you also have), but you don't want him to send it to you, then ask him for the hash value. If he sends you the correct hash value, then it is almost certain that he has that file. This is particularly useful in financial transactions, where you don't want a withdrawal of $100 to turn into a withdrawal of $1000 somewhere in the network. Normally, you would use a one-way hash function without a key, so that anyone can verify the hash. If you want only the recipient to be able to verify the hash, then read the next section.

Message Authentication Codes

A **message authentication code** (MAC), also known as a data authentication code (DAC), is a one-way hash function with the addition of a secret key (see Section 18.14). The hash value is a function of both the pre-image and the key. The theory is exactly the same as hash functions, except only someone with the key can verify the hash value. You can create a MAC out of a hash function or a block encryption algorithm; there are also dedicated MACs.

2.5 Communications Using Public-Key Cryptography

Think of a symmetric algorithm as a safe. The key is the combination. Someone with the combination can open the safe, put a document inside, and close it again. Someone else with the combination can open the safe and take the document out. Anyone without the combination is forced to learn safecracking.

In 1976, Whitfield Diffie and Martin Hellman changed that paradigm of cryptography forever [496]. (The NSA has claimed knowledge of the concept as early as 1966, but has offered no proof.) They described **public-key cryptography**. They used two different keys—one public and the other private. It is computationally hard to deduce the private key from the public key. Anyone with the public key can encrypt a message but not decrypt it. Only the person with the private key can decrypt the message. It is as if someone turned the cryptographic safe into a mailbox. Putting mail in the mailbox is analogous to encrypting with the public key; anyone can do it. Just open the slot and drop it in. Getting mail out of a mailbox is analogous to decrypting with the private key. Generally it's hard; you need welding torches. However, if you have the secret (the physical key to the mailbox), it's easy to get mail out of a mailbox.

Mathematically, the process is based on the trap-door one-way functions previously discussed. Encryption is the easy direction. Instructions for encryption are the public key; anyone can encrypt a message. Decryption is the hard direction. It's made hard enough that people with Cray computers and thousands (even millions) of years couldn't decrypt the message without the secret. The secret, or trapdoor, is the private key. With that secret, decryption is as easy as encryption.

This is how Alice can send a message to Bob using public-key cryptography:

(1) Alice and Bob agree on a public-key cryptosystem.

For example, the DiskLock program for Macintosh (version 2.1), sold at most software stores, claims the security of DES encryption. It encrypts files using DES. Its implementation of the DES algorithm is correct. However, DiskLock stores the DES key with the encrypted file. If you know where to look for the key, and want to read a file encrypted with DiskLock's DES, recover the key from the encrypted file and then decrypt the file. It doesn't matter that this program uses DES encryption—the implementation is completely insecure.

Further information on key management can be found in [457,98,1273,1225, 775,357]. The following sections discuss some of the issues and solutions.

8.1 GENERATING KEYS

The security of an algorithm rests in the key. If you're using a cryptographically weak process to generate keys, then your whole system is weak. Eve need not cryptanalyze your encryption algorithm; she can cryptanalyze your key generation algorithm.

Reduced Keyspaces

DES has a 56-bit key. Implemented properly, any 56-bit string can be the key; there are 2^{56} (10^{16}) possible keys. Norton Discreet for MS-DOS (versions 8.0 and earlier) only allows ASCII keys, forcing the high-order bit of each byte to be zero. The program also converts lowercase letters to uppercase (so the fifth bit of each byte is always the opposite of the sixth bit) and ignores the low-order bit of each byte, resulting in only 2^{40} possible keys. These poor key generation procedures have made its DES ten thousand times easier to break than a proper implementation.

Table 8.1 gives the number of possible keys with various constraints on the input strings. Table 8.2 gives the time required for an exhaustive search through all of those keys, given a million attempts per second. Remember, there is very little time differential between an exhaustive search for 8-byte keys and an exhaustive search of 4-, 5-, 6-, 7-, and 8-byte keys.

All specialized brute-force hardware and parallel implementations will work here. Testing a million keys per second (either with one machine or with multiple machines in parallel), it is feasible to crack lowercase-letter and lowercase-letter

Table 8.1
Number of Possible Keys of Various Keyspaces

	4-Byte	5-Byte	6-Byte	7-Byte	8-Byte
Lowercase letters (26):	460,000	$1.2 \cdot 10^7$	$3.1 \cdot 10^8$	$8.0 \cdot 10^9$	$2.1 \cdot 10^{11}$
Lowercase letters and digits (36):	1,700,000	$6.0 \cdot 10^7$	$2.2 \cdot 10^9$	$7.8 \cdot 10^{10}$	$2.8 \cdot 10^{12}$
Alphanumeric characters (62):	$1.5 \cdot 10^7$	$9.2 \cdot 10^8$	$5.7 \cdot 10^{10}$	$3.5 \cdot 10^{12}$	$2.2 \cdot 10^{14}$
Printable characters (95):	$8.1 \cdot 10^7$	$7.7 \cdot 10^9$	$7.4 \cdot 10^{11}$	$7.0 \cdot 10^{13}$	$6.6 \cdot 10^{15}$
ASCII characters (128):	$2.7 \cdot 10^8$	$3.4 \cdot 10^{10}$	$4.4 \cdot 10^{12}$	$5.6 \cdot 10^{14}$	$7.2 \cdot 10^{16}$
8-bit ASCII characters (256):	$4.3 \cdot 10^9$	$1.1 \cdot 10^{12}$	$2.8 \cdot 10^{14}$	$7.2 \cdot 10^{16}$	$1.8 \cdot 10^{19}$